Refine Search

Search Results -

Terms	Documents
(file$ near5 sharing and (server$ or network$ or distributed) and table$ and search$ near5 engine$).clm.	1

Database: US Pre-Grant Publication Full-Text Database
US Patents Full-Text Database
US OCR Full-Text Database
EPO Abstracts Database
JPO Abstracts Database
Derwent World Patents Index
IBM Technical Disclosure Bulletins

Search: L5

Refine Search | Recall Text | Clear | Interrupt

Search History

DATE: Saturday, October 23, 2004 Printable Copy Create Case

Set Name side by side	Query	Hit Count	Set Name result set
DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; PLUR=YES; OP=OR			
L5	(file$ near5 sharing and (server$ or network$ or distributed) and table$ and search$ near5 engine$).clm.	1	L5
L4	(file$ near5 sharing and (server$ or network$ or distributed) and table$ and search$ near5 engine$).ab.	0	L4
L3	(file$ near5 sharing and (server$ or network$ or distributed) and table$ and search$ near5 engine$).ti.	0	L3
L2	file$ near5 sharing and (server$ or network$ or distributed) and table$ and search$ near5 engine$	196	L2
L1	file$ near5 sharing same (server$ or network$ or distributed) same table$ same search$ near5 engine$	0	L1

END OF SEARCH HISTORY

h e b b cg b e e ch

Hit List

Clear | Generate Collection | Print | Fwd Refs | Bkwd Refs | Generate OACS

Search Results - Record(s) 1 through 1 of 1 returned.

☐ 1. Document ID: US 20040181667 A1

Using default format because multiple data bases are involved.

L5: Entry 1 of 1 File: PGPB Sep 16, 2004

PGPUB-DOCUMENT-NUMBER: 20040181667
PGPUB-FILING-TYPE: new
DOCUMENT-IDENTIFIER: US 20040181667 A1

TITLE: Secure streaming container

PUBLICATION-DATE: September 16, 2004

INVENTOR-INFORMATION:

NAME	CITY	STATE	COUNTRY	RULE-47
Venters, Carl Vernon III	Wilmington	NC	US	
Phillips, Eugene B. II	Raleigh	NC	US	
Ornstein, Seth	Silver Spring	MD	US	

US-CL-CURRENT: 713/164

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw De

Clear | Generate Collection | Print | Fwd Refs | Bkwd Refs | Generate OACS

Terms	Documents
(file$ near5 sharing and (server$ or network$ or distributed) and table$ and search$ near5 engine$).clm.	1

Display Format: - Change Format

Previous Page Next Page Go to Doc#

h e b b g e e e f e ef b e

L5: Entry 1 of 1 File: PGPB Sep 16, 2004

DOCUMENT-IDENTIFIER: US 20040181667 A1
TITLE: Secure streaming container

CLAIMS:

We claim:

1: A method of providing streaming content, comprising the steps of: creating a digital container that includes contents including streaming media content and digital rights management (DRM); selecting one or more modules for inclusion in the digital container, the selection of the modules being based on one at least one of a type of streaming media content and the DRM; encrypting the streaming media content of the digital container to produce a secured streaming container (SSC); and transmitting the SSC to a target device for access of the SSC from the target device.

2: The method of claim 1, wherein the transmitting includes transmitting the SSC over at least one of a local area network, a wide-area network, a wireless network, and the Internet.

3: The method of claim 1, wherein the target device includes one of a cell phone, a personal data assistant (PDA), a personal computer, a computing device, a portable music player, a tablet computer, a cable modem, satellite receiver, a television, and a cable television tuner.

4: The method of claim 1, wherein the digital container is created by receiving input of at least one of the target device, one or more media files to be included in the digital container, a transaction option type, a digital rights management (DRM) option, a digital container graphic, and a search descriptor data.

5: The method of claim 4, wherein: the transaction option type includes a financial transaction type, a transaction update type, a transaction update address, a server address, demographics type, or a subscription type; the financial transaction type includes at least a credit card type; and the subscription type includes at least a financial transaction defining a period of time.

6: The method of claim 4, wherein the creating step includes selecting one or more software modules based on a type of the one or more media files, which control the streaming of the one or more media files in the environment of the target device.

7: The method of claim 4, wherein the digital container graphic is either a static image and an animated image and is at least one of informational and promotional graphics that appears on a viewable electronic digital container cover before and after the digital container is opened.

8: The method of claim 1, further comprising encoding the streaming media content

for playback by one of a media player resident on the target device and a media player included with the digital container.

9: The method of claim 1, wherein the streaming media content includes at least one of video, audio, animation, and text content.

10: The method of claim 1, wherein the streaming media content is one or more streaming media files.

11: The method of claim 1, further comprising the step of creating one or more secondary files for inclusion in the digital container, the one or more secondary files include at least one of a hypertext markup language (html) file, an image file, and a segment of the one or more media files.

12: The method of claim 11, wherein the segment is at least one of: (i) viewable prior to executing a purchase transaction for the media content, and (ii) unencrypted for previewing.

13: The method of claim 12, wherein the at least one of an html file and image file are viewable during playing of the one or more streaming files.

14: The method of claim 1, further comprising the step of providing an execution batch file in the digital container for controlling presentation of the streaming media content in at least one of a preset sequence, a relative sequence, and a timing interval.

15: The method of claim 14, further comprising the step of establishing limits on access to the streaming media content based on at least one of a period of time and a number of access instances.

16: The method of claim 15, wherein the establishing limits includes limiting at least one of copying the streaming media content and transferring the streaming media content.

17: The method of claim 1, further comprising the step of producing informational and search metadata tag sets wherein the tag sets are included in the SSC.

18: The method of claim 17, wherein the tag sets are unencrypted extensible markup language (XML) tags.

19: The method of claim 18, wherein the tag sets are used by search engines to discover at least one of the digital container and the streaming media content.

20: The method of claim 18, wherein the XML tags are manually created.

21: The method of claim 18, wherein the XML tags describe at least a portion of the streaming media content and provides at least one of a file size and a file type.

22: The method of claim 18, wherein the XML tags provide access rights data to the target device.

23: The method of claim 18, wherein the XML tags provide at least one of a content file title, a key word data, and a key phrase data as search descriptors for search engines.

24: The method of claim 18, wherein the XML tags are substantially compliant with one of Open Mobile Alliance standard (OMA) and Open Data Rights language (ODRL) standard.

25: The method of claim 1, further comprising the step of registering the SSC with

a digital container verification database including one of identifying the SSC and providing date information about the SSC.

26: The method of claim 25, wherein the registering the SSC occurs automatically when the SSC is created.

27: The method of claim 1, wherein the transmitting step is via email, file transfer protocol (FTP), download from a web-site, peer-to-peer file sharing, instant messaging, or physical transport.

28: The method of claim 1, further comprising the step of encoding the digital container for transmission as a hypertext markup (HTML) file.

29: The method of claim 1, further comprising the step of establishing a transaction type that is to be executed for a user to gain permission to open the SSC, and when executed, the transaction type includes at least one of a password, demographic information, device information, financial data, credit card data, and personal user data.

30: The method of claim 29, wherein the personal identification includes at least one of a user identification number, a company identification number, and a biometric identification.

31: The method of claim 30, wherein the biometric information includes at least one of a voice data, a fingerprint data, a retina data, and a physical attribute scan data.

32: The method of claim 29, wherein the device information includes gathering data from a removable storage media.

33: The method of claim 29, wherein the transaction type includes a subscription transaction type that, when executed, gathers subscription data enabling a user to purchase multiple digital containers.

34: The method of claim 33, wherein the subscription transaction type gathers subscription data enabling a user to purchase the multiple digital containers related to a pre-determined time period.

35: The method of claim 1, wherein the encrypting step includes compressing the contents of the digital container.

36: The method of claim 1, wherein in the encrypting step a hidden key is incorporated into the digital container.

37: A method of receiving electronic data, comprising the steps of: receiving a secured streaming container (SSC) having streaming media content; and accessing the SSC to acquire portions of the streaming media content while other portions of the streaming media content remain secure in the SSC.

38: The method of claim 37, further comprising playing the portions of the streaming media content while other portions remain secured in the SSC.

39: The method of claim 37, wherein the SSC includes digital rights management (DRM) which controls the access to the SSC.

40: The method of claim 37, wherein the receiving step receives the SSC on a target device.

41: The method of claim 40, wherein the target device includes at least one of a cell phone, a personal data assistant (PDA), a personal computer, a computing

device, a portable music player, a tablet computer, a cable modem, a cable television tuner, and a satellite receiver.

42: The method of claim 40, wherein at least some of the contents of the SSC is configured to execute within the environment of the target device.

43: The method of claim 37, further comprising the step of obtaining permission to access the SSC.

44: The method of claim 43, wherein the obtaining permission includes at least one of (i) verifying a password, (ii) gathering demographic data, (iii) gathering personal data, (iv) gathering of the target device identification data, (v) processing a subscription transaction, and (vi) processing a financial transaction.

45: The method of claim 44, wherein the personal data includes at least one of a user identification (ID), a company ID, and a biometric data.

46: The method of claim 44, wherein the target device identification data includes at least one of an input from a removable storage media and an input provided from a secure device attached to a target device.

47: The method of claim 37, wherein in the accessing step, extensible markup language tags (XML) are read to determine at least one of a content file title, a digital rights management descriptor, a file size and a file type.

48: The method of claim 37, further including decrypting the SSC.

49: The method of claim 48, wherein the decrypting includes decompressing the streaming media content.

50: The method of claim 48, further including decoding the streaming media content as a hyper-text markup language (html) file.

51: The method of claim 37, further including the step of downloading a java applet in order to read the SSC content.

52: The method of claim 37, further comprising the step of supplying a password for a subsequent SSC access.

53: The method of claim 37, further comprising the steps of: successfully gaining permission to the SSC on a target device; sending a portion of data which is unique to the target device to a verification server; combining the portion of data and a digital container identification data previously registered to produce a permission token; sending the permission token to the target device; and rekeying an original key sent with the SSC using the permission token to securely rekey the streaming media content so that decrypting the streaming media content is locked to and performed only on the target device.

54: The method of claim 37, wherein the accessing step further includes: detecting an attempt to access the SSC; determining if permission has been previously granted to open the SSC and, if not, supplying transaction information; sending the transaction information to a digital container verification server in an encrypted session; sending a permission token back to the SSC; and granting permission to open the SSC.

55: The method of claim 54, wherein transaction information comprises supplying at least one of a financial information, a personal data, and a demographic data.

56: The method of claim 55, wherein the financial information is credit card

information.

57: The method of claim 55, wherein the personal data is at least one of a biometric data, a personal identification, and a password.

58: A method of creating and accessing streaming content, comprising the steps of: creating a digital container that includes contents including at least streaming media content and digital rights management (DRM); selecting one or more modules for inclusion in the digital container based on one at least one of a type of streaming media content and the DRM; encrypting the streaming media content and optionally the DRM to produce a secured streaming container (SSC); and accessing the secured streaming container (SSC) using the one or more modules to control playback of the streaming media content.

59: The method of claim 58, further comprising the steps of transmitting the SSC to a target device.

60: The method of claim 59, wherein the target device includes one of a cell phone, a personal data assistant (PDA), a personal computer, a computing device, a portable music player, a tablet computer, a cable modem, and a cable television tuner.

61: The method of claim 58, wherein the digital container is created by receiving input of at least one of a target device type, one or more media files to be included in the digital container, transaction option type, digital rights management (DRM) options, digital container graphics, and search descriptor data.

62: The method of claim 61, wherein: the transaction option type includes a financial transaction type, a transaction update type, a transaction update address, a server address, demographics type, a subscription type, the financial transaction type includes at least a credit card type, and the subscription type includes at least a financial transaction defining a period of time.

63: The method of claim 58, further comprising the step of selecting one or more modules based on the type of one or more media files and associated with the streaming media content, the one or more modules controlling the streaming of the one or more media files in the environment of the target device type.

64: The method of claim 58, further comprising encoding the streaming media content which is encoded for playback by one of a media player resident on a target device and a media player included with the digital container.

65: The method of claim 58, wherein the streaming media content includes at least one of video, audio, animation, and text.

66: The method of claim 58, further comprising providing an execution batch file in the digital container for controlling the presentation of the streaming media content in at least one of a preset sequence, a relative sequence, and a timing interval.

67: The method of claim 58, further comprising controlling access to the streaming media content using the DRM on subsequent accesses.

68: The method of claim 58, further including the steps of: decrypting the streaming media content; and playing the streaming media content using a media player.

69: The method of claim 58, wherein the accessing step further includes: detecting an access attempt to the SSC; determining if permission has been previously granted to open the SSC and, if not, supplying transaction information; sending the

transaction information to a digital container verification server in an encrypted session; sending a permission token back to the SSC; and granting permission to open the SSC.

70: The method of claim 58, further comprising the step of playing the streaming media content such that one or more segments of the streaming media content are sequentially played from the digital container while remaining portions of the streaming media content remain secure in the digital container until sequentially played.

71: A computer program product comprising a computer usable medium having readable program code embodied in the medium, the computer program product includes at least one component to: create a digital container that includes contents including streaming media content and digital rights management (DRM); select one or more modules for inclusion in the digital container wherein the selection of the modules is based on at least one of a type of streaming media content and the DRM; encrypt the streaming media content of the digital container to produce a secured streaming container (SSC); and transmit the SSC to a target device for access of the SSC from the target device.

72: The computer program product of claim 71, wherein the at least one component transmits the SSC over at least one of a local area network, a wide-area network, a wireless network, and the Internet.

73: The computer program product of claim 71, wherein the at least one component transmits to the device, the device being one of a cell phone, a personal data assistant (PDA), a personal computer, a computing device, a portable music player, a tablet computer, a cable modem, a satellite receiver, a television, and a cable television tuner.

74: The computer program product of claim 71, wherein the at least one component creates the digital container by receiving input of at least one of a target device type, one or more media files to be included in the digital container, a transaction option type, a digital rights management (DRM) option, a digital container graphic, and a search descriptor data.

75: The computer program product of claim 74, wherein: the transaction option type includes a financial transaction type, a transaction update type, a transaction update address, a server address, demographics type, a subscription type, the financial transaction type includes at least a credit card type, and the subscription type includes at least a financial transaction defining a period of time.

76: The computer program product of claim 71, wherein the at least one component selects one or more software modules based on the type of the one or more media files, the one or more software modules adapted to control the streaming of the one or more media files in the environment of the target device type.

77: The computer program product of claim 74, wherein the digital container graphic is either a static image and an animated image and is at least one of informational and promotional graphics that appears on a viewable electronic digital container cover before and after the digital container is opened.

78: The computer program product of claim 71, wherein the at least one component encodes the streaming media content and is encoded for playback by one of a media player resident on the target device and a media player included with the digital container.

79: The computer program product of claim 71, wherein the streaming media content includes at least one of video, audio, animation, and text content.

80: The computer program product of claim 71, wherein the streaming media content is one or more streaming media files.

81: The computer program product of claim 71, wherein the at least one component creates one or more secondary files for inclusion in the SSC, the one or more secondary files include at least one of a hypertext markup language (html) file, an image file, and a segment of the one or more media files.

82: The computer program product of claim 81, wherein the segment is at least one of: (i) viewable prior to executing a purchase transaction for the media content, and (ii) unencrypted for previewing.

83: The computer program product of claim 81, wherein the at least one of an html file and image file are viewable during playing of the one or more streaming files.

84: The computer program product of claim 71, wherein the at least one component provides an execution batch file in the digital container for controlling the presentation of the media content in at least one of a preset sequence, a relative sequence, and a timing interval.

85: The computer program product of claim 84, wherein the at least one component establishes limits on access to the media content based on at least one of a period of time and a number of access instances.

86: The computer program product of claim 85, wherein the establishing limits includes limiting at least one of copying the media content and transferring the media content.

87: The computer program product of claim 71, wherein the at least one component produces informational and search metadata tag sets and includes the tag sets in the SSC.

88: The computer program product of claim 87, wherein the tag sets are unencrypted extensible markup language (XML) tags.

89: The computer program product of claim 88, wherein the tag sets are used by search engines to discover at least one of the digital container and the streaming media content.

90: The computer program product of claim 88, wherein the XML tags are manually created.

91: The computer program product of claim 88, wherein the XML tags describe a least a portion of the streaming media content and provides at least one of a file size and a file type.

92: The computer program product of claim 88, wherein the XML tags provide access rights data to the device.

93: The computer program product of claim 88, wherein the XML tags provide at least one of a content file title, a key word data, and a key phrase data as search descriptors for search engines.

94: The computer program product of claim 93, wherein the XML tags are substantially compliant with one of Open Mobile Alliance standard (OMA) and Open Data Rights language (ODRL) standard.

95: The computer program product of claim 71, wherein the at least one component

registers the SSC with a digital container verification database including at least one of identifying the SSC and providing date information about the SSC.

96: The computer program product of claim 95, wherein the registering the SSC automatically occurs when the SSC is created.

97: The computer program product of claim 71, wherein the at least one component transmits using email, file transfer protocol (FTP), download from a web-site, peer-to-peer file sharing, instant messaging, or physical transport.

98: The computer program product of claim 71, wherein the at least one component encodes the digital container for transmission as a hypertext markup (HTML) file.

99: The computer program product of claim 71, wherein the at least one component establishes a transaction type that is to be executed for a user to gain permission to open the SSC, and when executed, the transaction type includes at least one of a password, demographic information, device information, gathering financial data, credit card data, and personal user data.

100: The computer program product of claim 99, wherein the personal identification includes at least one of a user identification number, a company identification number, and a biometric identification.

101: The computer program product of claim 100, wherein the biometric information includes at least one of a voice data, a fingerprint data, a retina data, and a physical attribute scan data.

102: The computer program product of claim 99, wherein the device information includes gathered data from a removable storage media.

103: The computer program product of claim 99, wherein the transaction type includes a subscription transaction type that, when executed, gathers subscription data enabling a user to purchase multiple digital containers.

104: The computer program product of claim 103, wherein the subscription transaction type, that when executed, gathers subscription data enabling a user to purchase the multiple digital containers related to a pre-determined time period.

105: The computer program product of claim 71, wherein the at least one component compresses the contents of the digital container.

106: The computer program product of claim 71, wherein the at least one component incorporates a hidden key into the digital.

107: A computer program product comprising a computer usable medium having readable program code embodied in the medium, the computer program product includes at least one component to: receive a secured streaming container (SSC) having streaming media content; and access the SSC to acquire portions of the streaming media content while other portions of the streaming media content remain secure in the SSC.

108: The computer program product of claim 107, wherein the at least one component plays the portions of the streaming media content while other portions remain secure n the SSC.

109: The computer program product of claim 108, wherein the at least one component receives the SSC on a target device.

110: The computer program product of claim 109 wherein at least some of the contents of the SSC is configured to execute within the environment of the target

device.

111: The computer program product of claim 110, wherein the target device includes at least one of a cell phone, a personal data assistant (PDA), a personal computer, a computing device, a portable music player, a tablet computer, a cable modem, a television, a cable television tuner, and a satellite receiver.

112: The computer program product of claim 107, wherein the at least one component obtains permission to access the SSC.

113: The computer program product of claim 112, wherein the permission is obtained using at least one of (i) verifying a password, (ii) demographic data, (iii) personal data, (iv) target device identification data, (v) processing a subscription transaction, and (vi) processing a financial transaction.

114: The computer program product of claim 113, wherein the personal data includes at least one of a user identification (ID), a company ID, and a biometric data.

115: The computer program product of claim 113, wherein the target device identification data includes at least one of an input from a removable storage media and an input provided from a secure device attached to the target device.

116: The computer program product of claim 107, wherein the at least one component reads extensible markup language tags (XML) to determine at least one of a content file title, a digital rights management descriptor, a file size and a file type.

117: The computer program product of claim 107, wherein the at least one component decrypts the SSC.

118: The computer program product of claim 107, wherein the at least one component decompresses the streaming media content.

119: The computer program product of claim 118, the at least one component decodes the streaming media content as a hyper-text markup language (html) file.

120: The computer program product of claim 107, wherein the at least one component downloads a java applet in order to read the contents of the SSC.

121: The computer program product of claim 107, wherein the at least one component requires a password for subsequent SSC access.

122: The computer program product of claim 107, wherein the at least one component: successfully gains permission to the SSC on a target device; sends a portion of data uniquely associated with the target device to a verification server; combines the portion of data and a digital container identification data previously registered with the verification server to produce a permission token, sends the permission token to the target device; and rekeys an original key sent with the SSC using the permission token to securely rekey the streaming media content so that decrypting the streaming media content is locked to and performed only on the target device.

123: The computer program product of claim 108, wherein the at least one component: detects an attempt to access the SSC; determines if permission has been previously granted to open the SSC and, if not, supplies transaction information; sends the transaction information to a digital container verification server in an encrypted session and the digital container verification server sends a permission token back to the SSC; and the at least one component grants permission to open the SSC.

124: The computer program product of claim 123, wherein the transaction information includes at least one of a financial information, a personal data, and a

demographic data.

125: The computer program product of claim 124, wherein the financial information is credit card information.

126: The computer program product of claim 124, wherein the personal data is biometric data.

127: The computer program product of claim 108, wherein the at least one component plays the streaming media content from a location on a target device so that the streaming media content plays without interruption avoiding network connectivity delays and disruptions.

128: The computer program product of claim 127, wherein the at least one component requires a password to replay the streaming media content.

129: The computer program product of claim 108, wherein the streaming media content is protected and cannot be copied.

130: A method of receiving information comprising the steps of: receiving a secured streaming container (SSC) having streaming media content; accessing the SSC using management controls; and playing the streaming media content on a target device wherein the streaming media content by-passes non-volatile memory or persistent storage.

131: A streaming media apparatus, comprising: a means for controlling access to a digital container having streaming media content; a means for securely streaming the streaming media content from the digital container once access is obtained to the digital container; and a means for playing the streaming media content such that one or more segments of the streaming media content are sequentially presented to a media player from the digital container while remaining segments of the streaming media content remain secure in the digital container until sequentially played.

132: The streaming media apparatus of claim 131, wherein streaming media content is one or more encrypted files of streaming media content and the means for securely streaming includes a means for streaming the one or more encrypted files of streaming media content so that the one or more files are invulnerable to copying or unauthorized access.

Previous Doc Next Doc Go to Doc#